UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/772,843	10/12/2004	Conor Cahill	AOL.0095	6050

22862 7590 04/15/2008

GLENN PATENT GROUP
3475 EDISON WAY, SUITE L
MENLO PARK, CA 94025

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
04/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/772,843	CAHILL ET AL.	
	Examiner	Art Unit	
	CANH LE	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/04/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the application filed on 02/04/2004.

Claims 1-23 have been examined and are pending.

Information Disclosure Statement

The information disclosure statement filed 02/04/2004 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because there is no copy for some references (X, Y, Z, aa, bb, cc, dd, ee, and ff). It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 21 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 21, the claim recites the limitation "if ***a same service provider,***" (emphasis added). This is vague in reference to what respect of the service provider to be considered as "a same service provider."

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-7, 9-12, 17-23 are rejected under 35 U.S.C. 102(e) as being anticipated by **Hinton** (US 2006/0048216 A1).

As per claim 1:

Hinton teaches a method for establishing an affiliation within a single sign-on system, comprising the steps of:

(a) defining a group of service providers that act as a single entity on a network for purposes of any of authentication, federation, and authorization **[fig. 2A, a group of service providers are enterprise B 206 and enterprise C 208; par. [0092], lines 18-32; "Assuming that the transaction requires some type of operation by enterprise**

206 and enterprise 204 during the course of transaction ....the identity provider and the service provider"];

(b) defining an owner of said affiliation that is responsible for maintaining a list that shows which service providers are members of said affiliation, as well as any control structure or meta-data associated with said affiliation **[fig. 2A, enterprise A 204, home domain/identity provider; par. [0086], "An enterprise has its own user registry and maintains relationships with its own set of rules"; par. [0092], lines 12-28; "user 202 initiates a transaction through a request for a protected resource at enterprise 204. If user 202 has been authenticated by enterprise 204 or will eventually be authenticated by enterprise 204 during the course of a transaction, then enterprise 204 is home the user's home, i.e. the user's identity provider, for this federated session. Assuming that the transaction requires some type of operation by enterprise 206 and enterprise 204 transfers an assertion to enterprise 206..."; par. [0093], lines 4-13; "The identity provider maintains authentication credentials, which may be physical supported by the user's employer, the user's ISP, or some other commercial entity..."; par. [0095]; fig. 4; par. [00164]; "Domain 410 becomes the user's identity provider or home domain for the duration of the user's federated session"; fig. 6, par. [0209]];** and

(c) providing a unique identifier for each affiliation within said single sign-on system in which said affiliation is defined **[par. [0176]; "a user is provided with a common unique user identifier across federation partners, which enables single-sign-on and the retrieval of attributes (if necessary) about amuser as part of the**

fulfillment of a request at one federation partner"; par. [0275], lines 5-11].

As per claim 2:

Hinton further teaches the method of claim 1, wherein said network comprises: a web services-based service infrastructure in which users manage sharing of is their personal information across identity providers and service providers **[fig. 2B, Web service client 224; fig. 2A, enterprise A 204 (identity provider), enterprise B 206 (service provider), and enterprise C 208 (service provider); par. [0092], lines 8-32; par. [0093], lines 4-13; par. [0094]- [0095]].**

As per claim 3:

Hinton further teaches the method of claim 2, wherein said web services implement a lightweight protocol for exchange of information in a decentralized, distributed environment **[par. [0103], lines 4-11; "Browser application 216 may also support plug-ins, such as web services client 224, and/or downloadable applets, which may or may not require a virtual machine runtime environment. Web services client 224 may use Simple Object Access Protocol (SOAP), which is a lightweight protocol for defining the exchange of structured and typed information in a decentralized, distributed environment"].**

As per claim 4:

Hinton further teaches the method of claim 3, wherein said protocol comprises:

an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses **[par. [0103], lines 11-16;SOAP is an XML-based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it; a set of encoding rules for expressing instances of application-defined datatypes; and a convention for representing remote procedure calls and responses"].**

As per claim 5:

Hinton teaches an apparatus for establishing an affiliation within a single sign-on system, comprising:

(a) a plurality of principals that can acquire a federated identity and be authenticated and vouched for by an identity provider **[fig. 2A; user 202, enterprise A 204; par. [0092], lines 8-1; "fig. 2A illustrates that the present invention supports the transitivity of trust and the transitivity of the authentication assertion process; a domain can issue an assertion based on its trust in an identity as asserted by another domain. User 202 initiates a transaction through a request for a protected resource at enterprise 204. If user 202 has been authenticated by enterprise 204 or will eventually be authenticated by enterprise 204 during the course of a transaction, then enterprise 204 is the user's home domain, i.e. the user's identity provider, for this federated session"; par. [0101], lines 5-6; "A**

federated environment includes federated entities that provide a variety of services for users"; par. [0089]; "the present invention also concerns a federated identity management system that establishes a foundation in which loosely coupled authentication, user enrollment, user profile management and/or authorization services, collaborate across security domains...A single-sign-on experience is established once a user establishes their participation in a federation"];

(b) an identity provider for authenticating and vouching for principals **[fig. 2A; user 202, enterprise A 204; par. [0092], lines 8-1; "fig. 2A illustrates that the present invention supports the transitivity of trust and the transitivity of the authentication assertion process; a domain can issue an assertion based on its trust in an identity as asserted by another domain. User 202 initiates a transaction through a request for a protected resource at enterprise 204. If user 202 has been authenticated by enterprise 204 or will eventually be authenticated by enterprise 204 during the course of a transaction, then enterprise 204 is the user's home domain, i.e. the user's identity provider, for this federated session"; par. [0101], lines 5-6; "A federated environment includes federated entities that provide a variety of services for users"; par. [0089]; "the present invention also concerns a federated identity management system that establishes a foundation in which loosely coupled authentication, user enrollment, user profile management and/or authorization services, collaborate across security**

domains…A single-sign-on experience is established once a user establishes their participation in a federation"];

(c) a plurality of service providers that act as a single entity with regard to authentication, federation and authorization to establish a single sign-on system within which such affiliation cooperates **[fig. 2A; user 202, enterprise A 204; par. [0092], lines 8-1; "fig. 2A illustrates that the present invention supports the transitivity of trust and the transitivity of the authentication assertion process; a domain can issue an assertion based on its trust in an identity as asserted by another domain. User 202 initiates a transaction through a request for a protected resource at enterprise 204. If user 202 has been authenticated by enterprise 204 or will eventually be authenticated by enterprise 204 during the course of a transaction, then enterprise 204 is the user's home domain, i.e. the user's identity provider, for this federated session"; par. [0101], lines 5-6; "A federated environment includes federated entities that provide a variety of services for users"; par. [0089]; "the present invention also concerns a federated identity management system that establishes a foundation in which loosely coupled authentication, user enrollment, user profile management and/or authorization services, collaborate across security domains…A single-sign-on experience is established once a user establishes their participation in a federation"; Service providers are enterprise B 206 and enterprise C 208]**;

(d) and at least one service associated with each service provider which comprises a grouping of common functionality comprising at least one method that

callers can use to manipulate information managed by said service with regard to a particular principal [**par. [0092], lines 8-1; "fig. 2A illustrates that the present invention supports the transitivity of trust and the transitivity of the authentication assertion process; a domain can issue an assertion based on its trust in an identity as asserted by another domain. User 202 initiates a transaction through a request for a protected resource at enterprise 204. If user 202 has been authenticated by enterprise 204 or will eventually be authenticated by enterprise 204 during the course of a transaction, then enterprise 204 is the user's home domain, i.e. the user's identity provider, for this federated session"]**.

As per claim 6:

This claim has limitations that are similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

As per claim 7:

This claim has limitations that are similar to those of claims 2-4, thus it is rejected with the same rationale applied against claims 2-4 above.

As per claim 9:

Hinton teaches a method for establishing an affiliation within a single sign-on system, comprising the steps of:

(a) defining a group of service providers that act as a single entity on a network for purposes of any of authentication, federation, and authorization **[fig. 2A, a group of service providers are enterprise B 206 and enterprise C 208; par. [0092], lines 18-32; "Assuming that the transaction requires some type of operation by enterprise 206 and enterprise 204 during the course of transaction ....the identity provider and the service provider"]**;

(b) providing a plurality of principals that can acquire a federated identity and be authenticated and vouched for by an identity provider **[fig. 2A; user 202, enterprise A 204; par. [0092], lines 8-1; "fig. 2A illustrates that the present invention supports the transitivity of trust and the transitivity of the authentication assertion process; a domain can issue an assertion based on its trust in an identity as asserted by another domain. User 202 initiates a transaction through a request for a protected resource at enterprise 204. If user 202 has been authenticated by enterprise 204 or will eventually be authenticated by enterprise 204 during the course of a transaction, then enterprise 204 is the user's home domain, i.e. the user's identity provider, for this federated session"; par. [0101], lines 5-6; "A federated environment includes federated entities that provide a variety of services for users"; par. [0089]; "the present invention also concerns a federated identity management system that establishes a foundation in which loosely coupled authentication, user enrollment, user profile management and/or authorization services, collaborate across security domains...A single-sign-on**

experience is established once a user establishes their participation in a federation"]; and

(c) providing an identity provider for authenticating and vouching for principals **[fig. 2A; user 202, enterprise A 204; par. [0092], lines 8-11; "fig. 2A illustrates that the present invention supports the transitivity of trust and the transitivity of the authentication assertion process; a domain can issue an assertion based on its trust in an identity as asserted by another domain. User 202 initiates a transaction through a request for a protected resource at enterprise 204. If user 202 has been authenticated by enterprise 204 or will eventually be authenticated by enterprise 204 during the course of a transaction, then enterprise 204 is the user's home domain, i.e. the user's identity provider, for this federated session"; par. [0101], lines 5-6; "A federated environment includes federated entities that provide a variety of services for users"].**

As per claim 10:

Hinton teaches further teaches the method of claim 9, further comprising the steps of:

(a) a principal logging into said identity provider **[fig. 2A; user 202, enterprise A 204; par. [0089]; par. [0091]-[0096]; par. [0156], lines 6-10; "A session can be defined as the set of transactions from (and including) the initial user authentication, i.e. logon, to logout. Within a session, a user's actions will be governed in part by the privileges granted to the user for that session"];**

(b) said principal visiting a first service provider and federating to said group **[fig. 2A; user 202, enterprise A 204 (identity provider), enterprise B 206 and enterprise C 208; par. [0091]-[0096]]**; and

(c) said principal then visiting any other service provider within said group **[fig 2A; enterprise B 206 and enterprise C 208; par. [0091]-[0096]].**

As per claim 11:

Hinton teaches the method of claim 9, further comprising the step of:

defining an owner of said affiliation that is responsible for maintaining a list that shows which service providers are members of said affiliation, as well as any control structure or meta-data associated with said affiliation **[fig. 2A, enterprise A 204, home domain/identity provider; par. [0086], "An enterprise has its own user registry and maintains relationships with its own set of rules"; par. [0092], lines 12-28; "user 202 initiates a transaction through a request for a protected resource at enterprise 204. If user 202 has been authenticated by enterprise 204 or will eventually be authenticated by enterprise 204 during the course of a transaction, then enterprise 204 is home the user's home, i.e. the user's identity provider, for this federated session. Assuming that the transaction requires some type of operation by enterprise 206 and enterprise 204 transfers an assertion to enterprise 206..."; par. [0093], lines 4-13; "The identity provider maintains authentication credentials, which may be physical supported by the user's employer, the user's ISP, or some other commercial entity..."; par. [0095]; fig. 4;**

par. [00164]; "Domain 410 becomes the user's identity provider or home domain for the duration of the user's federated session"; fig. 6, par. [0209]].

As per claim 12:

Hinton further teaches the method of claim 9, further comprising the step of:

providing a unique identifier for each affiliation within said single sign-on system in which said affiliation is defined **[par. [0176]; "a user is provided with a common unique user identifier across federation partners, which enables single-sign-on and the retrieval of attributes (if necessary) about amuser as part of the fulfillment of a request at one federation partner"; par. [0275], lines 5-11]**.

As per claim 17:

Hinton further teaches the method of claim 9, wherein said group has an identifier that is unique within a single sign-on system in which said group is defined **[fig. 2A, a group of service providers are enterprise B 206 and enterprise C 208; par. [0092], lines 18-32; "Assuming that the transaction requires some type of operation by enterprise 206 and enterprise 204 during the course of transaction ....the identity provider and the service provider"; [par. [0176]; "a user is provided with a common unique user identifier across federation partners, which enables single-sign-on and the retrieval of attributes (if necessary) about amuser as part of the fulfillment of a request at one federation partner"; par. [0275], lines 5-11]]**.

As per claim 18:

Hinton further teaches the method of claim 9, wherein service providers within a single sign-on system may be members of multiple groups, but can only act with a single affiliation for any given transaction **[par. [0086], lines 14-18; "Hence, within this federated environment, an authentication scheme allows for a single-sign-on experience within the rapid evolving heterogeneous environment in information technology"; par. [0087]; fig. 2A, a group of service providers are enterprise B 206 and enterprise C 208; par. [0092], lines 18-32; "Assuming that the transaction requires some type of operation by enterprise 206 and enterprise 204 during the course of transaction ....the identity provider and the service provider"]**

As per claim 19:

Hinton further teaches the method of claim 9, wherein a user federating with a group automatically federates with all members of said group **[par. [0087], lines 1-4; fig. 2A; par. [0092]; lines 12-32; "user 202 initiates a transaction through a request for a protected resource at enterprise 202. ...Assuming that the transaction requires some type of operation by enterprise 206 and enterprise 204 transfers an assertion to enterprise 206... Assuming that the transaction requires further operations such that enterprise 206 transfer an assertion to enterprise 208, then enterprise 206 is the issuing domain with respect to the requested operation..."**;

par. [0086], lines 9-12; "User can be granted access to resources at any of the federated enterprises as if they had a direct relationship with each enterprise"].

As per claim 20:

Hinton further teaches the method of claim 9, wherein a user authorizing access to a service by said federation authorizes access to any member of said group **par. [0092]; lines 12-32; "user 202 initiates a transaction through a request for a protected resource at enterprise 202. ...Assuming that the transaction requires some type of operation by enterprise 206 and enterprise 204 transfers an assertion to enterprise 206... Assuming that the transaction requires further operations such that enterprise 206 transfer an assertion to enterprise 208, then enterprise 206 is the issuing domain with respect to the requested operation..."; A user can be granted access to resources (i.e. enterprise 206 or enterprises 208) through identity provider 204; par. [0086], lines 9-12; "User can be granted access to resources at any of the federated enterprises as if they had a direct relationship with each enterprise"].**

As per claim 21:

Hinton further teaches the method of claim 9, further comprising the step of: providing a unique identifier for any service provider/group affiliation. wherein if a same service provider using a same service provider identity requests an identity of a user through different group affiliations, said service provider receives different, unique identifiers for

each group affiliation **[par. [0176]; fig. 2A; enterprise A, enterprise B, and enterprise C are known as unique identifiers].**

As per claim 22:

Hinton further teaches the method of claim 9, further comprising the step of: providing a same identifier to all members of said group when they are acting as a part of said group affiliation **[par. [0176]; unique user identifier of the user in anonymous manner].**

As per claim 23:

Hinton further teaches the method of claim 9, further comprising the step of: providing an affiliation name identifier for allowing sites to handle an automatic federation that take place with all members of said group **[par. [0176]; unique user identifier of the user in anonymous manner].**

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8 and 13-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Hinton** (US 2006/0048216 A1) in view of **David Booth** et al., "Web Service Architecture, W3C Working Group Note 11 February 2004", February 11, 2004, pp 1-98.

As per claim 13:

Hinton is silent about a discovery service for enabling a web service consumer to discover service information regarding a user's personal web services.

However, Booth teaches providing a discovery service for enabling a web service consumer to discover service information regarding a user's personal web services **[pg. 46-47, 2.3.3.3 Discovery Service section; "...The primary role of discovery service is to facilitate the discovery of Web service...Human may interact with the discovery service through an appropriate software, such as a browser..."; pg. 69, fig. 4; "The discovery service somehow obtains both the Web service description ("WSD" in figure 3-2 [p. 68]) and an associated functional description ("FD") of the service"].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify/combine the method of Hinton by including the teaching of Booth because it would facilitate the process of finding an appropriate provider agent for a particular task **[Booth, pg. 46-47, 2.3.3.3 Discovery Service section].**

As per claim 14:

Booth further teaches the method of claim 13, further comprising the step of: providing a web service consumer associated with a service provider for requesting a service descriptor and assertion for service from said discovery service and for presenting an assertion from said other service provider with affiliate information **[pg. 49-50, 2.3.3.6 Resource description section; "A resource description is any machine readable data that may permit resources to be discovered. Resource descriptions may be of many different form, tailored for specific purpose, but all resource descriptions must contain the resource's identifier ... A resource description are used by and within discovery services [p.46] to permit agents to discover the resource..."].**

As per claim 15:

Booth further teaches the method of claim 14, further comprising the step of: said discovery service checking said other service provider affiliation and generating a service assertion based upon said other service provider affiliation **[pg. 68-70; 3.4 Web Service Discovery; fig. 4; "b) The requester entity supplies criteria to the discovery service to select a Web service description ...c)The discovery service returns one or more Web service description (or references to them) that meet the specified criteria. If multiple service descriptions are returned, the requester entity selects one, perhaps using additional criteria"].**

As per claim 16:

Booth further teaches the method of claim 15, further comprising the step of: said web service consumer invoking a service with said service assertion via a web service provider **[pg. 6, 1.1 Purpose of the Web Service Architecture section; "Web service provide a standard means of interoperating between different software applications, running on a variety of platform and/or frameworks... The WSA provides a conceptual model and a context for understanding Web services and the relationships the components of this model"; pg. 7-9, 1.4 What is a Web service section; fig 1-1, The general process of Engaging a Web service].**

As per claim 8:

This claim has limitations that are similar to those of claim 13, thus it is rejected with the same rationale applied against claim 13 above.

Conclusion

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

US 20050154913 A1 to Barriga, Luis et al.;

US 20070130343 A1 to Pardo-Blazquez; Avelina et al.;

US 20060155993 A1 to Biswas; Kamalendu et al.;

US 20050177730 A1 to Davenport, Christopher J. et al.;

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Canh Le/
Examiner, Art Unit 2139

April 10, 2008
/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139